

2012

Abused Internet Domain
Registration Analysis for
Calculating Risk and Mitigating
Malicious Activity

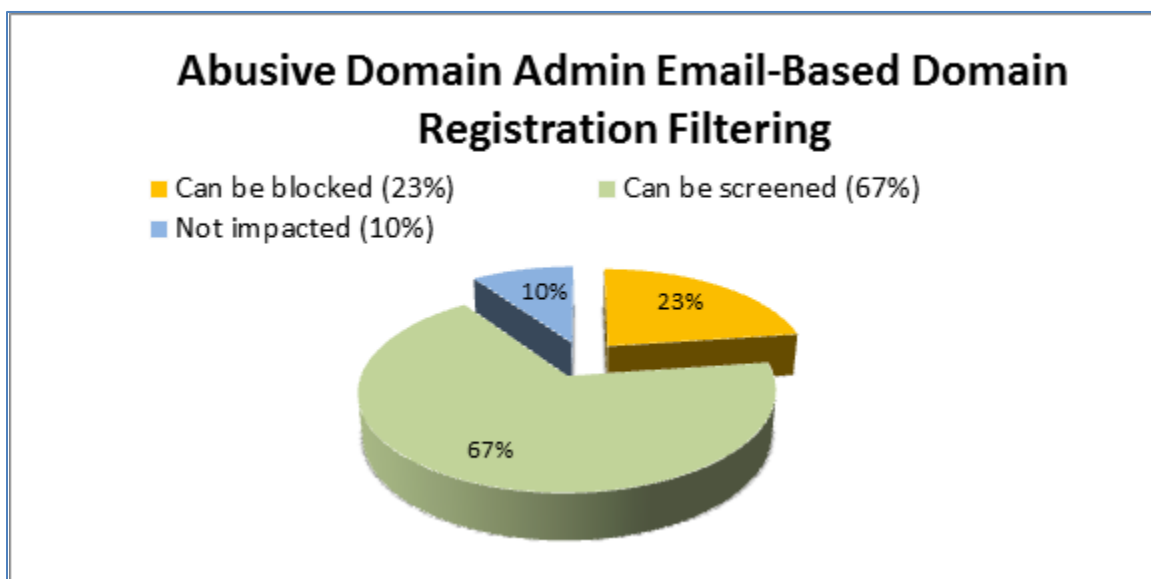
KnjOn.com LLC

Brief Version

2/18/2012

Promising Research

KnjOn.com LLC is proud to release this briefing of our Abused Internet Domain Registration Analysis for Calculating Risk and Mitigating Malicious Activity. KnjOn reviewed nearly one million WHOIS records from domain names advertised with spam in 2011 and found that 22.8% of the rogue registrations could be blocked with fundamental validation. Another 67.5% could be filtered or held for additional screening with a robust analysis developed in response to our findings. This study focused exclusively on the Administrator Email Address in each WHOIS record. We are confident that this promising method could prevent slightly more than 90% of truly abusive registrations, potentially curtailing the 14 million distinct spam instances which supplied the test data. In the real world those instances are duplicated and repeated for Internet users globally creating the unwanted traffic and related criminality which plague us daily. In our research we separated the domains which were spoofed or hijacked to focus purely on ones which were created specifically as illicit shopping sites or for malware distribution.



Abusive Registrations Are Preventable

The problem for domain name Registrars has always been inability to predict user intent and the belief that any screening would increase domain cost and slow the registration process. We now know this is not the case and that statistical analysis with a vast repository of intelligence can be used to mitigate abusive registrations. To be clear, this is not a blacklist. Rather, this is a two-part process which uses existing policy-based rules to handle the smaller percentage of obvious violations and a comprehensive analytics engine to assign risk factors to the larger portion of potential abuses. While the ICANN Registrar Accreditation Agreement¹ requires accurate information² and validation³, in practice this has been a challenge. Fortunately, it appears this can be done with relative ease. Registrars expend significant resources now dealing with spam and abuse after the fact when it is often too late.

¹ <http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm>

² <http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3.3.1.7>

³ <http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3.7.8>

Addressing a Serious Issue

The annual cost of spam to companies and individuals is in the tens of billions of dollars⁴ as well as wasting the precious time of employees⁵. Malware (viruses, Trojans, etc.) presents an ever-evolving threat to industry as well as personal Internet use⁶ as it expands into mobile devices. The world of spam and Internet abuse is a complex place involving a variety of players and resources⁷. However, the use of domain names by illicit parties is a critical and final piece of the cycle. The outer edges of Internet abuse (spam email, malware distribution, server compromises, etc.) are fleeting and constantly changing in source. But even illicit businesses require a certain amount of stability. Domain names as transaction platforms provide a critical resource to people selling rogue pharmaceuticals, counterfeit products, or illicit services. Without access to domain names the underground Internet would be much harder to operate.

Moving from the Elementary to the Complex

As shown above, 23% of abusive domains could be blocked for basic policy reasons. These abusive registrations, not hijacked or spoofed spam domains, contained obvious errors which would have invalidated the domain WHOIS record. The set includes even typographical errors which make the administrator email address unreachable. These represent attempts to obfuscate or make the domain operators unaccountable. A further 67% of abusive domains can be filtered by analytics. Within this range there are a number of subtle and discrete factors which allowed us to identify risky domain registrations.

Assigning Risk

The Internet Corporation of Assigned Names and Numbers (ICANN) and their contracted parties (Registries and Registrars) are sustained on the high volume trade in domain names. Consumers of domain names expect speed, convenience and value in their purchases. The competition to provide easy and rapid domain deployment among Registrars has also created opportunities to exploit the system. It is not generally in the interest of the Registrar or ICANN to deny a registration as it is impossible to discern user intent, but it is possible to assign risk based accumulated data.

Validated 15 Factors Based on Knowledge Repository

By compiling everything learned from the 2011 abuse data KnujOn was able to create a test engine which caught potentially abusive registrations. The series of comprehensive tests completed in microseconds and would be transparent to the registrant.

The Abuse Range “Sweet Spot”

There is a major difference between compromised domains and domains specifically registered for illicit traffic. To the victim of spam or malware all abused domains appear to be the same. Within this study KnujOn was able to predict, through our analysis, which domains were created for spamming and which were hijacked in one way or another. This has allowed us to disregard the noise and focus on core illicit activity.

⁴ <http://www.meierhenrylaw.com/web/?p=2510>

⁵ <http://ridiculouslyefficient.com/2011/11/30/email-spam-costs/>

⁶ <http://www.slideshare.net/GFISoftware/viprebusinesssocialmediamalware-en-gen>

⁷ <http://edition.cnn.com/2011/BUSINESS/06/06/cybercrime.cost/index.html>

Examples of Missing Policy Enforcement

Some domains should never have existed. One of the registrations caught with an impossible email address was an illicit online pharmacy: md-pill.com. In further examining the WHOIS record we found the address and phone number for this purported “pharmacy” is actually contact information for newspaper *Los Angeles Times*. As can be seen below this is a “No Prescription” pharmacy which is illegal in most countries. The WHOIS record is outlined in red and the official contact information for the *Los Angeles Times* is outlined in black.

The image shows a screenshot of the website md-pill.com on the left and its WHOIS record on the right. The website features a banner with "No Prescription Needed" and "Buy generics - Save your money". The WHOIS record is highlighted with a red box and contains the following information:

```
Domain name: md-pill.com
Administrative Contact:
Marco Lopes Marco Lopes
+1.2132375000 fax: Fax:
202 W. 1st St.
Los Angeles
USA
```

To the right of the WHOIS record is a "Contact Us" section for the *Los Angeles Times*, with the following mailing address:

Los Angeles Times
Mailing Address:
202 W. 1st St.
Los Angeles, CA 90012
Phone: (213) 237-5000
Fax: (213) 237-7679

The purpose is to illustrate how simple “red flags” in one entry can lead to the discovery of an entire false record. Such a registration should have been held for secondary screening. Many abusive registrations also have incomplete administrator email addresses as in the example below:

```
Administrative Contact:
Qualified Prospect Center
Business Services (postmaster@qualifiedprospectcenter)
+1.2132860704
Fax: +7.2132860704
PO Box 37635
#94011 Ste: 2110
Philidelphia, PA 19101
US
```

Allowing this type of registration to pass will only cost the Registrar later in terms of dealing with complaints and other issues.

Invalid Privacy Services Draw Illicit Domain Registrants

In this study we also reviewed which WHOIS privacy protection services were most heavily used by abusive registrants and why. Some services are technically in violation of the ICANN contract and therefore offer additional concealment for illicit Internet commerce.

Illicit Domain Registrations vs. Abusive Administrator Email Domains

Our research results show that abusive registrants frequently have their “home base” at one Registrar and purchase domains to be exploited at a second Registrar. We have exposed the attack vectors of various malicious actors. The data also indicates why some Registrars have more abusive registrations.

What Else We Found

The results of this study were intriguing, revealing the complex relationships between abusive registrants and spammed domains. As in previous KnujOn studies on spam, we find the activity is clustered. In our study there were 956,702 unique abused domain names with 237,557 unique administrator email addresses in their registrations. These email addresses were at 71,484 unique administrator email address domains, but more than 55% of the abuse originated from just 50 administrator email domains. Within 500 of the worst administrator email domains we see 73% of the abuse. This percentage of abuse only rises to 77% at the 1000 worst administrator email domain mark. So, as we approach the larger population of abusive registrations the volume of abuse drops considerably. If we change the data view to specific unique abusive administrator email addresses we can isolate about 50% of the abusive registration activity to just 1144 specific domain administrators. Over seven million abuse instances examined in the study, one half of the total, can be attributed to these specific administrators.

Full Version of Research

KnujOn’s 30-page report on Abused Internet Domain Registration Analysis for Calculating Risk and Mitigating Malicious Activity contains detailed analysis, case studies, and fascinating findings. This is a proprietary work being used to develop a solution and is not part of a general public release. When complete, a fully developed a subscription-based API will be made available. If you are interested in this work please contact us: contact@knujon.com.

About Knujon

KnujOn is a unique Internet security and policy analysis project which works with ordinary Internet users, small businesses, governments, nonprofit organizations, and the global community of Internet policy developers to combat abuse, illicit activity, and in general enhance the overall Internet user experience. KnujOn has developed custom mathematical modeling techniques which expose not only where abuses are originating but why and what can be done. KnujOn has moved beyond blacklists to develop a multidimensional abuse response paradigm. Our process is concerned with dire policy failures and loopholes in the Internet architecture which have been exploited by malicious parties for their own benefit at the expense of consumers at large. Any questions or concerns can be directed to contact@knujon.com. More information at <http://www.knujon.com>.